Big data, privacy and cyber security breaches – why information governance is critical

Organisations globally are struggling to manage both the opportunities and risks posed by the explosion of data they hold, which is increasing at an exponential rate each year. Strong information governance is an effective way to maximise the opportunities arising from data mining and extract value from the data held. As well, effective implementation of clear policies and processes to minimise the risks arising from information held will result in cost efficiencies.

Where do the risks and costs arise?

The vast amounts of data held pose increased risks and costs to organisations, arising from:

- legal and compliance, particularly in relation to privacy obligations, with the growing focus on privacy arising from high-profile cyberattacks and thefts of customer records;
- information communication and technology (ICT) systems that prevent privacy and ICT security breaches;
- the cost of production of documents in litigation and regulatory investigations; and
- record and information management (RIM) complying with legal and business requirements, where data is increasing exponentially, and retention policies may not be keeping pace with business operations and legal requirements.

Who is responsible?

Typically, an organisation's data and information is managed by various 'owners' – for example:

- compliance – risk and compliance director or chief risk officer;
- eDiscovery/document production – eDiscovery counsel or general counsel;
- ICT security – chief technology officer or chief information officer;
- legal – general counsel;
- privacy – chief privacy officer or general counsel; and
- records and information management (RIM) – RIM manager.

What is information governance?

Information governance (IG) is defined as:

> The activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs.[1]

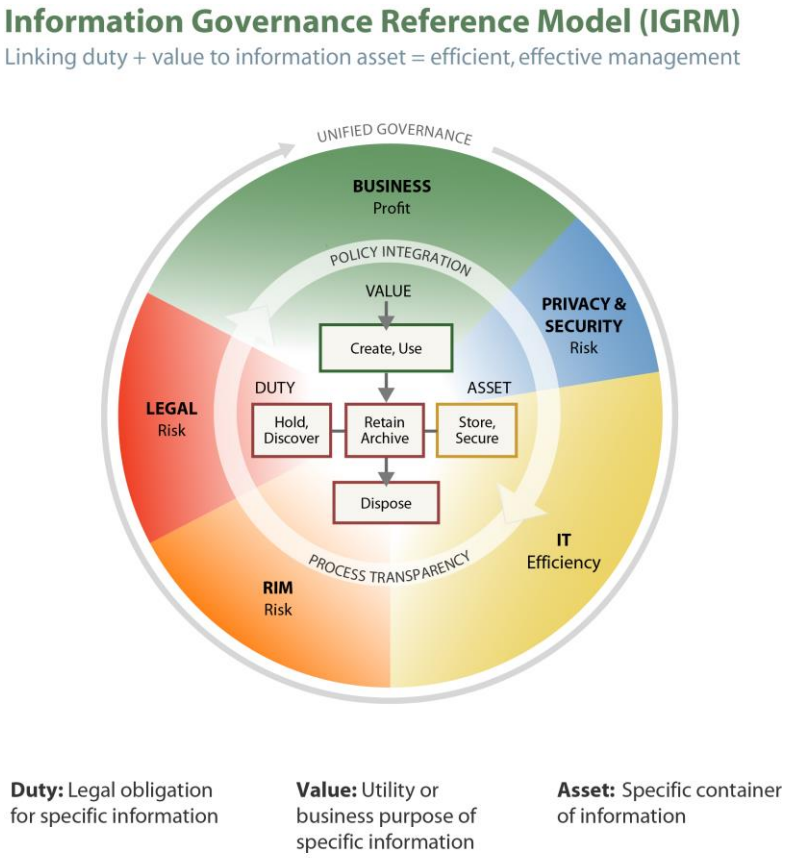
IG – a critical foundation for effective governance

The key to addressing and managing information/data throughout the organisation is to take a holistic approach that is driven from the board/CEO/C-suite level down.

[1] Information Governance Initiative Annual Report 2014.

A sound IG framework is the critical foundation that then enables organisations properly to govern and manage the information held. The benefits of a holistic approach to IG are:

- senior-executive-level engagement and decision-making on important strategic opportunities and risk mitigation issues concerning organisational information;
- improved management of data with more efficient retrievability of data retained;
- defensible destruction of redundant, outdated and trivial data/information with an audit trail that can be relied upon in litigation;
- improved selection and return on investment (ROI) on new technology, appropriate to the organisation's legal, compliance and business needs;
- comprehensive and aligned policies, processes and response plans – including comprehensive ICT security and privacy breach response plans; and
- reduced costs and increased efficiencies arising from the implementation of an aligned strategy and policies, in contrast to the inefficiencies of the traditional fragmented siloed approach.



Technology – tool and solution?

While the proliferation of data has been caused by technology, it is also technology that is providing rapidly evolving tools to manage the exponentially increasing data. However, technology is only part of the solution, as IG strategy, policies, processes, people and technology all need to be aligned, to deliver on the objective of maximising the value of the information and minimising risks and costs.

There is a rapidly growing market for technology solutions in the IG sphere for the wide spectrum of information management needs. And there are many technology options for managing ICT security, eDiscovery, RIM and compliance, etc. Types of technology that are dramatically changing the ways in which information is managed within organisations include:

- **Auto-classification** technology, enabling automatic identification, classification, retrieval, archival and disposal of information, based on an organisation's classification rules. This type of technology enables defensible disposal of data and should enable better adherence to IG policies.
- **Analytic** technology, which identifies relevant data and data patterns from large data sets. Analytics can be used across a number of the traditionally siloed areas within organisations. For example, analytics and relevance ranking are used extensively in discovery for litigation, and provide substantial cost and time savings. Analytics is used with traditional RIM as well as increasingly being used to better understand customers, so as to tailor products, and/or develop new products, with the ultimate aim of increasing profits.
- **eDiscovery** technology is increasingly being brought in-house by major organisations, as a way to increase efficiency and reduce costs by:
    - pre-litigation review of information, early case assessment and managing responses to regulatory investigations in-house; and
    - maintaining control over the data, preserving confidentiality and ensuring sensitive data is not removed from the organisation's network.

Technologies such as those outlined above should be selected and implemented within the context of the overarching IG strategy, policies and priorities.

Technology and privacy

One of the greatest challenges and risks facing organisations is dealing with privacy issues concerning data containing personally identifiable information, medical records and other sensitive details. Some organisations are proactively addressing privacy by embedding:

- privacy controls and mechanisms in ICT systems before they are implemented within an organisation – i.e., ensuring there is compliance with core organisational values and privacy obligations prior to implementation, which, in the longer term, is more cost efficient; and
- privacy lawyers in new product development teams, so that products not only meet legal obligations but are designed to meet the growing concerns about privacy and enable customers/users more control over the use of their information – e.g., with online social media products, allowing users to determine the level of privacy, which they may vary from time to time.

IG – is your organisation achieving best practice?

Whether information management achieves best practice, so that risks are minimised and the opportunities and value of information are maximised, comes down to four factors. Ask yourself:

- Are your leaders embedding IG as a foundation of good corporate governance?
- Do you have a clear and comprehensive IG framework with current policies and processes in place?
- Are those responsible for information management able to work collaboratively across functions to ensure that IG strategic objectives are met and achieve best practice with resulting efficiencies?
- Is data being used effectively for multiple business-value-creating purposes?

If the answer to any of these questions is 'no', there is probably an opportunity for greater alignment of the IG framework, policies, processes and people.

If you would like assistance reviewing your current IG ecosystem, please contact Susan Bennett, Principal, on +61 2 8226 8682 or email susan.bennett@sibenco.com.

This article is for reference purposes only and does not constitute legal advice.